

UNITED STATES DISTRICT COURT

JUN 29 2018

for the
Eastern District of Missouri

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

)
)
)
)
)
)

In the Matter of the Search of Information Associated with Dustin Boone
and cellular phone number [REDACTED] that is stored at premises
controlled by Apple, Inc.

) Case No. 4:18 MJ 1197 JMB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the NORTHERN District of CALIFORNIA
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal *(identify the person or describe the property to be seized):*

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before July 13, 2018 *(not to exceed 14 days)*
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

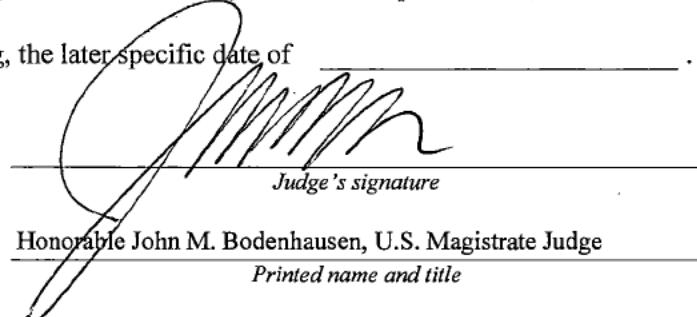
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to United States Magistrate Judge John M. Bodenhausen
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized *(check the appropriate box)*

for _____ days *(not to exceed 30)* until, the facts justifying, the later specific date of _____.

Date and time issued:

6/29/18 9:25 am


Judge's signature
Honorable John M. Bodenhausen, U.S. Magistrate Judge
Printed name and title

City and state: St. Louis, MO

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **Dustin Boone** cellular phone number [REDACTED] that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email

was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfofolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of inter alia, 18 U.S.C. §§ 241 and 242 involving Dustin Boone and all other SLMPD officers involved in the arrest or detention of Luther Hall and other individuals and the protests in downtown St. Louis, since September 15, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
 - b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
 - c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
 - d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;
 - e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts; and
 - f. Any and all records related to the arrest and detention and/or assault of Luther Hall or other individuals involved in the protests; any and all records related to the arrest and detention of individuals involved in the protests in downtown St, Louis; any records of communication between Dustin Boone and Luther Hall or other SLMPD officers; any and all communications with any individuals related to the aftermath and/or investigation into the arrest, detention, and assault of Luther Hall and other individuals during the protests in downtown St.

Louis, and any photographs and/or other video related to the protests and/or arrests and detention of individuals involved in the protests in downtown St. Louis.

Any and all records that may constitute evidence of crimes, wrongs, or other acts that may be admissible to prove motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident, or that may be admissible for any other purpose pursuant to Fed. R. Evid. 404(b).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, Inc., and my title is _____.

_____ I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple, Inc. The attached records consist of _____.

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, Inc., and they were made by Apple, Inc. as a regular practice; and

b. such records were generated by Apple, Inc. electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

UNITED STATES DISTRICT COURT

FILED

JUN 29 2018

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

In the Matter of the Search of Information Associated with Dustin Boone and
cellular phone number [REDACTED] that is stored at premises controlled by
Apple, Inc.

Case No. 4:18 MJ 1197 JMB

APPLICATION FOR A SEARCH WARRANT

I, Darren Boehlje, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the NORTHERN District of CALIFORNIA, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

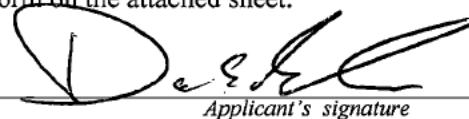
The search is related to a violation of:

*Code Section*18 USC § 241
18 USC § 242*Offense Description*Conspiracy Against Rights
Deprivation of Rights Under Color of Law

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

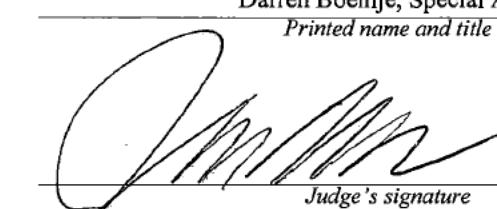
- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

Darren Boehlje, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/29/18

 Judge's signature

Honorable John M. Bodenhausen, U.S. Magistrate Judge

Printed name and title

City and state: St. Louis, MO

AUSA: Jennifer A. Winfield

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

In the Matter of the Search of Information
Associated with **Dustin Boone** and cellular
phone number [REDACTED] that is stored
at premises controlled by Apple, Inc.

Case No. 4:18 MJ 1197 JMB

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Darren Boehlje, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with **Dustin Boone** and cellular phone number [REDACTED] (hereafter “Account”) that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been so employed since 2011. I am presently assigned to the St. Louis Division of the FBI. My responsibilities include the investigation of federal crimes to include violations of Title 18 United States Code (U.S.C.) § 242 (Deprivation of Rights). I am currently assigned to investigate allegations of unreasonable force under color of law. I received over twenty-one weeks of specialized law enforcement training at the FBI Academy in Quantico, Virginia. My experience obtained as a Special Agent of the FBI has included investigations of multiple violations of federal criminal civil rights laws. I know cellular telephones are commonly used by law enforcement officers to communicate about arrests they have just made. Cellular telephones are also used by officers suspected of using unreasonable or excessive force to communicate with one another,

attempting to justify their actions or keep their actions hidden. Likewise, cellular phones are often used by such subjects to brag about or apologize for their actions. These cellular telephones and their respective cellular telephone service providers possess the capability to store and transmit data thereby aiding in determining the general location of a cellular telephone.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of inter alia, 18 U.S.C. §§ 241 (Conspiracy Against Rights) and 242 (Deprivation of Rights) have been committed by Dustin Boone, a police officer with the St. Louis Metropolitan Police Department (“SLMPD”) as well as other still-to-be-identified SLMPD officers. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

1. Following the acquittal of former SLMPD Officer Jason Stockley on a murder charge stemming from an officer-involved shooting on September 15, 2017, there were multiple days of concentrated protesting in and around St. Louis. SLMPD Officer Luther Hall, an African-American, 22-year veteran officer of SLMPD, was assigned to attend the protests and work in an undercover capacity, documenting protest activity and property destruction. After working for two days at the protests, Hall returned to his assignment at approximately 7:00 PM on September 17, 2017, to record protest activity. Hall and his partner, who was also undercover, were together until just after 8:00 PM, when they ran in separate directions after unidentified SLMPD officers fired numerous rounds of pepper balls, mace, and bean bag rounds into the crowd from their vehicles. Hall never heard an order to disperse prior to SLPMD’s deployment of these devices.

2. While Hall was at an intersection, SLMPD SUVs pulled up, and officers in tactical gear got out. A female officer told Hall to get to the ground. Hall raised his hands in surrender, his camera (a Nikon DSLR) in his left hand and his cell phone in his right hand, actively recording.

Hall was wearing a shirt that he wore specifically for this undercover activity, short and tight enough to show his weapon-less waistband when he raised his arms. As he was complying and getting to his knees, Hall felt himself being picked up from behind and then slammed to the ground face first. He was again picked up and slammed to the ground face first. As a result, Hall's face felt sticky and warm, which later turned out to be blood gushing from his nose and lip. While on the ground, officers repeatedly punched Hall with closed fists, hit him with sticks, and kicked him while wearing boots. Hall's hands were out in front of him on the ground. Although the officers were telling him to put his hands behind his back, he was unable to comply because officers were standing on his arms. Hall described it as a "free for all."

3. SLMPD officers ultimately placed Hall's hands behind his back, handcuffed him, and sat him up on the pavement next to a black male in custody who had an abrasion on his face and was wearing a Patriots shirt. While seated on the pavement, Hall felt pain in his back and neck and could see his nose was bleeding. In order to relieve some of his back pain, Hall leaned back, but each time he did so, the officer standing behind him, whom Hall possibly identified as Officer Randy Hays, "checked" Hall in the back with his knee and shin-guard, telling him to "stop fucking moving."

4. An SLMPD officer then removed the camera hanging around Hall's neck, removed the battery from the camera, and threw the camera onto the pavement, breaking it. Hall believes the officer removed the battery thinking the battery was the memory card. Hall also saw his cell phone on the ground with a circular imprint on the shattered screen. Hall believes the imprint was made by an officer's baton.

5. Hall did not want to reveal his true identity and instead looked around for someone he knew for help. He made eye contact with Civil Disobedience Team [REDACTED], with whom he was familiar. [REDACTED] enlisted the assistance of two SLMPD SWAT officers who then picked up Hall and took him to an SLMPD Bear vehicle, where Hall was provided medical treatment. [REDACTED] arrived and arranged for Hall to be transported from the scene in a police vehicle, as if he were being arrested in order to maintain Hall's undercover status. Hall was transported to SLMPD Headquarters where he reported to [REDACTED] that the officers "beat the fuck out of him like Rodney King." Hall then went

to a temporary medical facility that the Missouri State Highway Patrol (“MSHP”) had staged for police officers so that he could receive additional treatment.

6. Hall suffered significant injuries as a result of the assault. At the MSHP facility, he received three layers of stiches on his lip where there was an approximately one centimeter hole. His has since been diagnosed with multiple herniated discs. An injury to his jaw made it difficult for him to eat, and he subsequently lost approximately 15 pounds. He also recently had gallbladder surgery, which, according to Hall’s doctors, may have been precipitated by the stress of the assault.

7. SLMPD Internal Affairs Division investigator [REDACTED] interviewed Luther Hall on October 25, 2017. In that interview, Hall identified four officers as having been at the scene of his assault: Officers Bailey Colletta, Chris Myers, Randy Hays, and Dustin Boone, the officer whose cellular phone number is the subject of this affidavit. Additionally, FBI Special Agents Darren Boehlje, your affiant, and Jennifer Lynch, interviewed [REDACTED] on December 20, 2017. [REDACTED] stated that on September 18, 2017, at SLMPD’s staging area for the protest response teams, he announced that anyone who was involved in an arrest the night before at 14th St. and Olive St. should come see him. Officers Randy Hays, Dustin Boone, [REDACTED], and Chris Myers came to [REDACTED], identifying themselves as having been involved in the arrest of Luther Hall.

8. On Sunday, September 25, 2017, at 9:04 a.m., Hall received a text message from the phone number [REDACTED], the cellular phone number that is the subject of this affidavit. Hall provided a copy of the text message to federal authorities. The message states the following:

“Luther, this is Dustin Boone. I am sure you know by now that I was involved in the incident last Sunday downtown. I have attempted to reach out to you through a few different commanders and I have been told to hold off. I have not heard much from anyone in regard to you receiving the message I wanted to be conveyed to you so I decided to text you myself today. I feel like an apology will never be enough but I would really like to speak to you in person so I can apologize face to face as a man and not through a text message. I completely understand if you are not willing to meet with me and if that is the case, I would ask if you are willing to accept a phone call from me once you are healthy and feel the timing is right. Again, I would

much rather tell you I am sorry while standing in front of you than over the telephone, but understand your side of all of this as well. Please let me know and if you are willing I will be available at any point in time. I hope you are healing both physically and mentally. I can't imagine what you have go through this past week. I hope you will allow me the opportunity to tell you I am sorry in person, it won't make it right but I feel it is the least I can do. I hope to talk to you soon Luther. Get well."

9. On December 22, 2017, the *St. Louis American*, a newspaper, published an article titled, "Chief O'Toole Promotes White St. Louis Officer Who Allegedly Beat Black Undercover Cop during Stockley Verdict Protest Mass Arrest." That article named SLMPD Officers Dustin Boone, Randy Hays, and Joseph Marcantano, as part of the federal investigation into Hall's assault.

10. On January 2, 2018, a federal search warrant was authorized by the Honorable Patricia L. Cohen in Case Number 4:18MJ6003 PLC, for the Apple, Inc. account associated with cellular phone number [REDACTED], the cellular phone number that is the subject of this affidavit. Apple, Inc. produced data associated with the account through December 31, 2017. A review of the Apple, Inc. data produced revealed numerous text messages between Dustin Boone and other officers, including Randy Hays and Chris Myers, and family members concerning the assault on Luther Hall, in addition to the above-described message from Officer Boone to Luther Hall. For example, on September 18, 2017, the day after the assault, Boone and Hays exchanged text messages, which include but are not limited to the following text messages:

Boone: Everyone seems to think that we r ok. Still don't like it hanging over me tho!

Hays: Yeah, me either, just told [REDACTED] the ass whooping can be explained. The camera thing can't and we weren't apart of that.

Boone: Yes, trust me, I am WAY more alright with what u and I did than what the others did! I don't like that we put our hands on another cop, but the situation was a little fucked up too, wasn't JUST us.

Hays: Wasn't just us, I don't like the beating the hell outta a cop, but the department put him in that spot, he could've announced himself any time.

And he wasn't complying. The camera thing is just ignorant, nothing we all haven't done and if it was a protestor it wouldn't be a problem at all.¹

Boone: Correct

Other text messages found are evidence of Boone, and other officers' willfulness with respect to the violation of protestors', or perceived protesters', constitutional rights. For example, on September 15, 2017, the day the protests started, Dustin Boone texted: "The more the merrier!!! It's gonna get IGNORANT tonight!! But it's gonna be a lot of fun beating the hell out of these shitheads once the sun goes down and nobody can tell us apart!!!!" Also contained in the data produced by Apple, Inc. was the text message described above sent from Dustin Boone to Luther Hall on September 25, 2017.

11. On May 31, 2018, Magistrate Judge John Bodenhausen authorized a warrant to seize and search Dustin Boone's cellular phone in Case Number 4:18MJ1149 JMB.

12. During the morning of June 5, 2018, FBI Special Agent Darren Boehlje, your affiant, and Special Agent Robert Polanco approached Officer Boone regarding the instant investigation. Agents presented Officer Boone with a target letter to advise Boone that based upon this investigation it appears that he has criminal culpability in connection with the aforementioned incident.

13. Following contact with Officer Boone on June 5, 2018, investigators analyzed Pen Register Data for Officer Boone's phone number [REDACTED] from that day. The analysis revealed that on June 5, 2018, at 9:16 AM Officer Boone called [REDACTED] phone number [REDACTED] and the call lasted approximately 1:53 minutes. [REDACTED] with the St. Louis Metropolitan Police Department, [REDACTED], and a person with whom Officer Boone repeatedly discussed the aforementioned protest and the assault of Luther Hall, as seen in his previously obtained Apple, Inc. records. At 9:32 AM, [REDACTED] called Officer Boone and they spoke for approximately 3:04 minutes. At 10:21 AM, Officer Boone received a text message from Officer Myers phone number (314-540-3072) to which he responded immediately. Officer Myers then replied with a text message at 10:22 AM. Officer Myers texted Officer Boone at 1:31 PM to which Officer Boone responded immediately. Officer Boone then

¹ This text message was received in two texts, out of order, and was re-ordered here for ease of reading.

received another text from Officer Myers at 2:09 PM, to which Officer Boone did not respond. At 4:39 PM, Officer Boone received two incoming calls from Officer Myers. Officer Boone answered the second call and spoke to Officer Myers for approximately 4:39 minutes. At 8:01 PM, Officer Myers sent Officer Boone two text messages, and both went unanswered by Officer Boone.

14. On June 6, 2018, FBI Special Agent Darren Boehlje, your affiant, and Special Agent Robert Polanco approached Officer Boone to execute the May 31, 2018 warrant and seized Officer Boone's cellular phone associated with the aforementioned phone number. On that same date, Officer Myers called Officer Boone four times in a row (10:30 AM, 10:31 AM, 10:41 AM, and 10:42 AM), and Officer Hays called Officer Boone three times in a row (11:28 AM, 11:29:01 AM, 11:29:47 AM).

15. As evidenced by the above outlined communications between Officer Boone, [REDACTED] [REDACTED], Officer Myers, and Officer Hays, investigators surmise that there has been ongoing conversations via text message and cellular phone between various police officers, including but not limited to Officers Chris Myers and Randy Hays, [REDACTED], and Officer Boone regarding the aforementioned protest and the assault of Luther Hall.

16. A preservation request was sent and accepted by Apple, Inc. for **Dustin Boone** and cellular phone number [REDACTED] on December 21, 2017 and renewed on May 2, 2018.

INFORMATION REGARDING APPLE ID AND iCLOUD²

17. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

² The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "iCloud: iCloud storage and backup overview," available at <https://support.apple.com/kb/PH12519>; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

18. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

19. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

20. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

21. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and

utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

22. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

23. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

24. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”)

messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

25. The United States is investigating allegations that SLMPD Officer Dustin Boone and other unidentified SLMPD officers while acting under color of law, willfully deprived Luther Hall and others of the right to be free from unreasonable seizure, which includes the right to be free from unreasonable force, a right secured and protected by the Constitution and laws of the United States. The allegations disclose possible violations of, inter alia, 18 U.S.C. §§ 242 and 241. In my training and experience, and based on the prior Apple, Inc. warrant executed as part of this investigation, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

26. As stated above, Officer Boone used a cellular phone to make admissions about alleged offenses and maintained an iCloud account on which he stored his text messages and phone logs, among other content. Stored communications and files from the Account are vital to this ongoing investigation. For example, and as seen with the data that Apple, Inc. previously produced in this investigation for Officer Boone, the stored communications and files connected to Officer Boone's Apple ID are likely to provide direct evidence of the offenses under investigation. Based on my training and experience, including with this investigation, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

27. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-

location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

28. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

30. As stated above, the investigation to date, including the return from the first search warrant executed on Apple, Inc. for Officer Boone's account data, has revealed that Officer Boone maintains an Apple iCloud account in which he stores his text messages, phone logs, internet search history, photographs, and other information that constitutes evidence of the crimes under investigation. Given the information previously obtained from Officer Boone's Apple, Inc. account and his continued communications (including communications after receiving a target letter) that appear -- from the persons involved and timing -- to be related to the assault of Luther Hall, there is reason to believe that obtaining the Apple, Inc. data associated with Officer Boone's cellular phone account through the present will produce additional evidence of the crimes under investigation.

31. Additionally, based on my training and experience, I know that those who have committed crimes often delete incriminating evidence from their phones. Therefore, comparing the content of Officer Boone's physical phone, seized by investigators on June 6, 2018, to the

content of this Apple, Inc. account may produce evidence of Boone's consciousness of guilt and evidence of efforts to obstruct the law enforcement investigation into the assault of Luther Hall.

32. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

1. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple, Inc. to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

2. Based on the forgoing, I request that the Court issue the proposed search warrant.

3. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

4. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

5. The foregoing has been reviewed by Reginald Harris, Executive Assistant United States Attorney, U.S. Attorney's Office, Eastern District of Missouri and Fara Gold, Special Litigation Counsel, Criminal Section, Civil Rights Division, U.S. Department of Justice.

REQUEST FOR SEALING

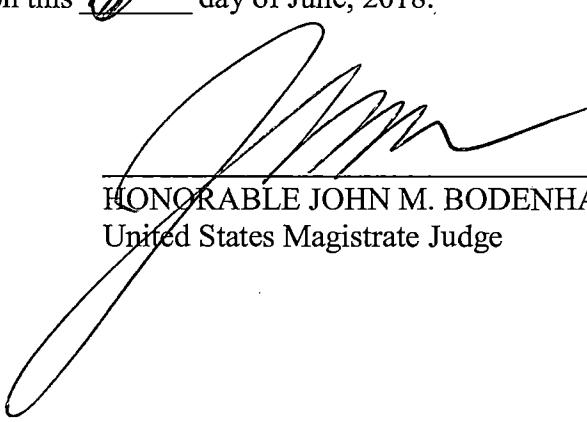
6. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Darren Boehlje, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 29/3 day of June, 2018.



HONORABLE JOHN M. BODENHAUSEN
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **Dustin Boone** cellular phone number [REDACTED] that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email

was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of inter alia, 18 U.S.C. §§ 241 and 242 involving Dustin Boone and all other SLMPD officers involved in the arrest or detention of Luther Hall and other individuals and the protests in downtown St. Louis, since September 15, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts; and
- f. Any and all records related to the arrest and detention and/or assault of Luther Hall or other individuals involved in the protests; any and all records related to the arrest and detention of individuals involved in the protests in downtown St, Louis; any records of communication between Dustin Boone and Luther Hall or other SLMPD officers; any and all communications with any individuals related to the aftermath and/or investigation into the arrest, detention, and assault of Luther Hall and other individuals during the protests in downtown St.

Louis, and any photographs and/or other video related to the protests and/or arrests and detention of individuals involved in the protests in downtown St. Louis.

Any and all records that may constitute evidence of crimes, wrongs, or other acts that may be admissible to prove motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident, or that may be admissible for any other purpose pursuant to Fed. R. Evid. 404(b).